# デバイスの追加と整理

この章は次のトピックで構成されています。



## Prime Infrastructure へのデバイスの追加

Cisco Prime Infrastructure はデバイス、ロケーション、およびポート グループを使用して、ネットワーク内の要素を整理します。デバイスをテーブルまたはマップ（ネットワーク トポロジ）で表示すると、デバイスは属しているグループを単位として整理されます。デバイスが Prime Infrastructure に追加されると、**Unassigned Group** という名前のグループに割り当てられます。その後、簡単な管理と設定のためのデバイス グループの作成 （25 ページ） で説明されているように、デバイスを目的のグループに移動できます。

（注） Prime Infrastructure は、Cisco 9k デバイスの Stackwise Virtual Link（SVL）をサポートしていません。

メモ **Catalyst 9800 シリーズ** デバイスが AP およびクライアントの運用データを Prime Infrastructure に送信するように指定するには、次のことを確認します。

- NETCONF-YANG をグローバルに有効にします。次を使用して設定できます。

```
device# conf t
device(config)# netconf-yang
```

- アクセスに SSH/Telnet を使用するデバイスを Cisco Prime Infrastructure で管理できる特権 *15* を持ったユーザがいます。以下を使用できます。

```
username cisco1 privilege 15 password 0 cisco1
```

- 次のコマンドを使用して AAA new-model を有効にします。

```
device(config)# aaa new-model
```

NETCONF-SSH 接続および edit-config 操作を設定します。

```
aaa authorization exec default local
```

- Prime Infrastructure がクライアントを検出できない場合は、デバイスでクライアントの検出に必要な以下の CLI を検証してください。

```
wireless client onboarding-event
```

（注） ASR 9900 のデバイス セットは、Prime Infrastructure によって効果的に監視されるように、**netconf agent tty** コマンドと **xml agent tty** コマンドを使用して設定する必要があります。

**表 *1*: デバイスの追加方法**

| サポートされているデバイスの追加方法 | 参照先： |
|---|---|
| 以下を使用してシード デバイスのネイバーを検出して複数のデバイスを追加する | ディスカバリを使用したデバイスの追加（3 ページ）。 |
| • Ping スイープと SNMP ポーリング（クイック ディスカバリ） | • クイック ディスカバリの実行 （5 ページ） |
| • カスタマイズされたプロトコル、クレデンシャル、およびフィルタ設定（ディスカバリ ジョブを繰り返す場合に便利） | • カスタマイズされたディスカバリ設定でのディスカバリの実行 （6 ページ） |
| CSV ファイルで指定された設定を使用して複数のデバイスを追加する | 他のソースからのデバイスのインポート（8 ページ） |

| サポートされているデバイスの追加方法 | 参照先： |
|---|---|
| 単一のデバイスを追加する（たとえば、新しいデバイス タイプの場合） | 手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （10 ページ） |

# ディスカバリ プロセスについて

Prime Infrastructure は、ディスカバリ プロセス中に次の手順を実行します。

1. ICMP ping を使用して、各デバイスが到達可能かどうかを確認します。Prime Infrastructure がデバイスに到達できない場合は、デバイスの到達可能性ステータスが [到達不能（Unreachable）] となります。
2. SNMP クレデンシャルを確認します。デバイスが ICMP で到達できるが、SNMP クレデンシャルが無効な場合は、デバイスの到達可能性ステータスが [Ping Reachable] となります。

   デバイスが ICMP および SNMP の両方で到達できる場合は、デバイスの到達可能性ステータスが [到達可能（Reachable）] となります。
3. Telnet および SSH のクレデンシャルを確認します。
4. Prime Infrastructure が必要な通知を受信できるように、デバイス設定を変更してトラップ レシーバを追加します。
5. インベントリ収集プロセスを開始して、すべてのデバイス情報を収集します。
6. **[インベントリ（Inventory）]** > **[ネットワークデバイス（Network Devices）]** ページにデバイスを追加します。

検出を実行した後、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択して、その検出が完了したことを確認します。

# ディスカバリを使用したデバイスの追加

Prime Infrastructure は、次の 2 つのディスカバリ方式をサポートしています。

- シード デバイスからの ping スイープ（クイック ディスカバリ）。デバイス名、SNMP コミュニティ、シード IP アドレス、およびサブネット マスクが必要です。クイック ディスカバリの実行 （5 ページ）を参照してください
- カスタマイズされたディスカバリ方法（ディスカバリ設定）の使用：設定を行い、今後ディスカバリを再実行する場合は、この方法をお勧めします。カスタマイズされたディスカバリ設定でのディスカバリの実行 （6 ページ）を参照してください。

（注）

- ディスカバリ ジョブが既存のデバイスを再検出し、デバイスの最後のインベントリ収集ステータスが [完了済み（Completed）] である場合、Prime Infrastructure は、既存のクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きしません。他のすべてのステータス（既存のデバイス上）の場合、Prime Infrastructure は、デバイスのクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きします。
- データベースのメンテナンス期間中に多数のデバイスが追加された場合、サービス検出に通常より時間がかかることがあります。したがって、夜間や週末には大規模な作業を回避することをお勧めします。
- 自律 AP がディスカバリ プロセスから除外され、検出時間が最適化されます。[デバイスのインポート（Import Devices）] または [クレデンシャルプロファイル（Credential Profile）] を使用して、自律 AP を手動で追加する必要があります。

デバイスのディスカバリ プロセスは、次に示す順序で実行されます。Prime Infrastructure はディスカバリの実行時に、デバイスの到達可能性状態（[到達可能（Reachable）]、[ping 到達可能（Ping Reachable）]、または [到達不能（Unreachable）]）を設定します。状態の詳細については、「デバイスの到達可能性状態と管理状態 （17 ページ）」を参照してください。

1. Prime Infrastructure は、ICMP ping を使用して、デバイスに到達可能であるかどうかを判別します。デバイスに到達できない場合、到達可能状態は [到達不能（Unreachable）] に設定されます。
2. サーバは、SNMP 通信が可能かどうかをチェックします。
   - ICMP がデバイスに到達可能で、SNMP 通信が不可能な場合、その到達可能性状態は [ping 到達可能（Ping Reachable）] に設定されます。
   - ICMP と SNMP の両方がデバイスに到達できる場合、その到達可能性状態は [到達可能（Reachable）] です。
3. デバイスの Telnet および SSH クレデンシャルが確認されます。クレデンシャルに障害が起きた場合は、障害に関する詳細が [ネットワークデバイス（Network Devices）] テーブルの [最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列に表示されます（たとえば、「**Wrong CLI Credentials**」など）。到達可能性の状態は変更されません。
4. Prime Infrastructure が SNMP を使用して必要な通知を受信できるように、デバイス設定が変更されて、トラップの受信者が追加されます。
5. インベントリ収集プロセスが開始され、すべてのデバイス情報が収集されます。
6. Web GUI にすべての情報（ディスカバリが完全に成功したか、部分的に成功したかなど）が表示されます。

（注） Prime Infrastructure がデバイスの SNMP 読み取り/書き込みクレデンシャルを検証すると、デバイス ログが更新され、Prime Infrastructure（IP アドレスで識別される）によって構成が変更されたことが示されます。

## 検出されたデバイスの管理 IP アドレス タイプ（IPv4/IPv6）の指定

検出されたデュアルホーム（IPv4/IPv6）デバイスでは、Prime Infrastructure が管理 IP アドレスとして IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを指定します。

**ステップ 1** **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [検出（Discovery）]** を選択します。

**ステップ 2** [管理アドレスに対する IPv4/IPv6 設定（IPv4/IPv6 Preference for Management Address）] ドロップダウンリストから [v4] または [v6] のいずれかを選択します。

**ステップ 3** [保存（Save）] をクリックします。

## クイック ディスカバリの実行

単一のシードデバイスを使用して ping スイープを実行する場合には、この方法を使用します。デバイス名、SNMP コミュニティ、シードの IP アドレスおよびサブネット マスクのみが必要です。構成管理機能の使用を計画している場合は、プロトコル、ユーザ名、パスワード、およびイネーブル パスワードを入力する必要があります。

[サービス（Services）] > [ネットワークサービス（Network Services）] > [ゲストユーザ（Guest Users）] の順に選択して、Prime Infrastructure によって検出されたゲスト ユーザを表示できます。検出後のゲスト ユーザ アカウントの正しいライフタイムを確認するには、デバイスに正しい時間設定が指定されていることを確認します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** の順に選択して、ウィンドウ右上の [クイック ディスカバリ（Quick Discovery）] リンクをクリックします。

**ステップ 2** 少なくとも、名前、SNMP コミュニティ、シードの IP アドレス、およびサブネット マスクを入力します。

**ステップ 3** [今すぐ実行（Run Now）] をクリックします。

### 次のタスク

結果を表示するには、[ディスカバリ ジョブ インスタンス（Discovery Job Instances）] 領域の、[ジョブ（Job）] ハイパーリンクをクリックします。

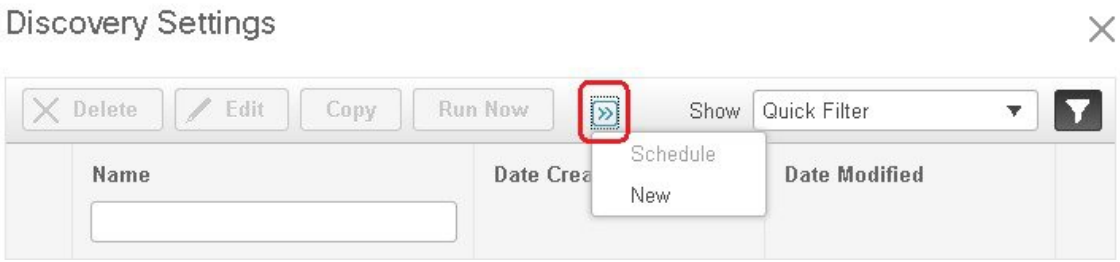
# カスタマイズされたディスカバリ設定でのディスカバリの実行

Prime Infrastructure は、ディスカバリ プロファイルを使用してネットワーク デバイスを検出できます。ディスカバリ プロファイルには、ネットワーク要素を検索し、それらに接続してインベントリを収集する方法を Prime Infrastructure に指示する設定のコレクションが含まれています。たとえば、Prime Infrastructure に CDP、LLDP、OSPF を使用してデバイスを検出することや、単純な ping スイープの実行を指示できます（ping スイープの結果の例は「ping スイープのサンプルの IPv4 IP アドレス （6 ページ）」に記載されています）。フィルタを作成して、コレクションの微調整、クレデンシャルセットの指定、およびその他のディスカバリ設定を行うこともできます。プロファイルは必要な数だけ作成できます。

プロファイルの作成後、プロファイルを使用するディスカバリ ジョブを作成し、実行します。ディスカバリジョブの結果は [ディスカバリ（Discovery）] ページで確認できます。ジョブをスケジュールして、定期的に実行を繰り返すこともできます。

**ステップ 1** [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）] を選択して、ウィンドウ右上の [ディスカバリ設定（Discovery Settings）] リンクをクリックします。（[ディスカバリ設定（Discovery Settings）] リンクが表示されない場合は、[クイックディスカバリ（Quick Discovery）] リンクの隣の矢印アイコンをクリックします）。

**ステップ 2** [検出設定（Discovery Settings）] ポップアップで、[新規（New）] をクリックします。




**ステップ 3** [ディスカバリ設定（Discovery Settings）] ウィンドウに設定を入力します。その設定に関する情報を取得するには、設定の隣にある [?] をクリックします。たとえば、[SNMPv2 クレデンシャル（SNMPv2 Credentials）] の横にある [?] をクリックすると、ヘルプのポップアップにプロトコルと必須の属性がすべて表示されます。

**ステップ 4** システムからディスカバリ設定をインポートするには、[インポート（Import）] ボタンをクリックします。

**ステップ 5** ディスカバリ設定を XML 形式でエクスポートするには、[エクスポート（Export）] ボタンをクリックします。

**ステップ 6** [今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行するか、[保存（Save）] をクリックして設定を保存し、後で実行するようにディスカバリをスケジュールします。

## ping スイープのサンプルの IPv4 IP アドレス

次の表に、ping スイープ結果の例を記載します。

| サブネット範囲 | ビット数 | IP アドレスの数 | サンプルのシード IP アドレス | 開始 IP アドレス | 終了 IP アドレス |
|---|---|---|---|---|---|
| 255.255.240.0 | 20 | 4094 | 205.169.62.11 | 205.169.48.1 | 205.169.63.254 |
| 255.255.248.0 | 21 | 2046 | 205.169.62.11 | 205.169.56.1 | 205.169.63.254 |
| 255.255.252.0 | 22 | 1022 | 205.169.62.11 | 205.169.60.1 | 205.169.63.254 |
| 255.255.254.0 | 23 | 510 | 205.169.62.11 | 205.169.62.1 | 205.169.63.254 |
| 255.255.255.0 | 24 | 254 | 205.169.62.11 | 205.169.62.1 | 205.169.63.254 |
| 255.255.255.128 | 25 | 126 | 205.169.62.11 | 205.169.62.1 | 205.169.63.127 |
| 255.255.255.192 | 26 | 62 | 205.169.62.11 | 205.169.62.1 | 205.169.63.62 |
| 255.255.255.224 | 27 | 30 | 205.169.62.11 | 205.169.62.1 | 205.169.63.30 |
| 255.255.255.240 | 36 | 18 | 205.169.62.11 | 205.169.62.1 | 205.169.63.14 |
| 255.255.255.248 | 29 | 6 | 205.169.62.11 | 205.169.62.9 | 205.169.63.14 |
| 255.255.255.252 | 30 | 2 | 205.169.62.11 | 205.169.62.9 | 205.169.63.10 |
| 255.255.255.254 | 31 | 0 | 205.169.62.11 | | |
| 255.255.255.255 | 32 | 1 | 205.169.62.11 | 205.169.62.11 | 205.169.62.11 |

# 検出の確認

検出が完了したら、プロセスが正常に完了したかどうかを確認できます。

ディスカバリの成功を確認するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [検出（Discovery）]** を選択します。

**ステップ 2** 詳細を表示するディスカバリジョブを選択します。

**ステップ 3** 左側のナビゲーション ペインから **[ユーザ ジョブ（User Jobs）] > [検出（Discovery）]** を選択し、特定のジョブを選択します。

**ステップ 4** **[ジョブ インスタンスの検出（Discovery Job Instances）]** の下で、矢印を展開して、検出されたデバイスの詳細を表示します。

デバイスが見つからない場合は、次を行います。

- ディスカバリ設定を変えてから、ディスカバリを再実行します。
- デバイスを手動で追加します。詳細については、「手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （10 ページ）」を参照してください。

[ディスカバリジョブインスタンス (Discovery Job Instances )] セクションに、**エクスポート**および**更新**ボタンが表示されます。ジョブ情報は PDF と CSV の両方としてエクスポートできます。

# 他のソースからのデバイスのインポート

デバイスのインポート元となる管理システムが他にある場合、またはすべてのデバイスとその属性がリストされたスプレッドシートをインポートする場合は、一括デバイス ファイルをインポートすることで、デバイス情報を Prime Infrastructure に追加できます。デバイスのインポート CSV ファイルの作成 （8 ページ）で説明するように、インポートする CSV ファイルが完全で、正しくフォーマットされていることを確認する必要があります。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択し、[ネットワーク デバイス（Network Devices）] テーブルの上にある + アイコンをクリックしてから、[一括インポート（Bulk Import）] を選択します。

**ステップ 2** [操作（Operation）] ドロップダウン リストから、[デバイス（Device）] を選択します。

**ステップ 3** [CSV ファイルの選択（Select CSV File）] の横にある [参照（Browse）] をクリックし、インポートするデバイスが含まれている CSV ファイルまで移動して選択します。

**ステップ 4** [インポート（Import）] をクリックします。

**ステップ 5** **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [ユーザ ジョブ（UserJobs）] > [デバイスの一括インポート（Device Bulk Import）]** を選択して、インポートのステータスを確認します。

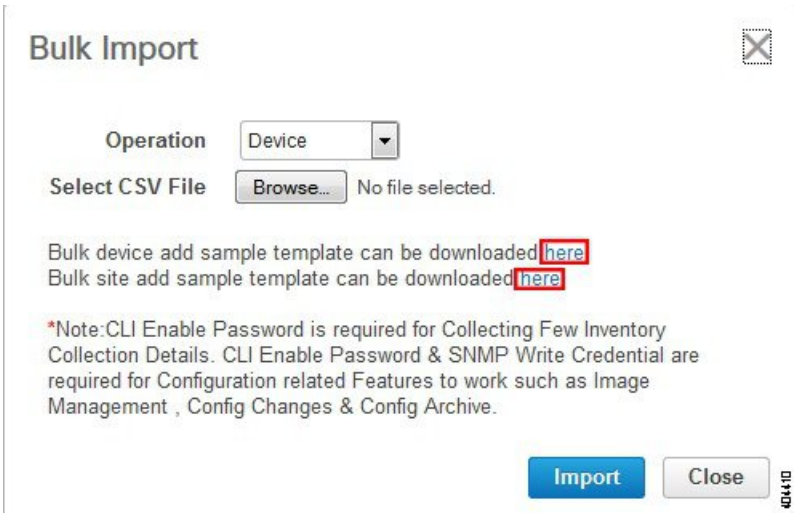
**ステップ 6** 矢印をクリックして、ジョブの詳細を展開し、インポート ジョブの詳細と履歴を表示します。

# デバイスのインポート CSV ファイルの作成

CSV ファイルを使用してデバイスを別のソースから Prime Infrastructure にインポートする場合は、デバイス テンプレートを使用して CSV ファイルを準備する必要があります。このテンプレートは、次のように Prime Infrastructure からダウンロードできます。

1. **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** [インベントリ（Inventory）] > [デバイス管理（Device Management）] > を選択します。次に、[一括インポート（Bulk Import）] をクリックします。

2. [一括デバイス追加サンプルテンプレートをダウンロードできます（Bulk device add sample template can be downloaded）] の横にある [ここ（here）] リンクをクリックします（下の図でハイライト表示されています）。テンプレートには、インポートする予定の CSV デバイス ファイルに含める必要がある情報のすべてのフィールドと説明が含まれています。




CSV ファイルをインポートしてデバイスを追加する場合は、Prime Infrastructure がこれらのデバイスを管理できる範囲は、CSV ファイルで指定した情報によって異なることに注意してください。たとえば、CSV ファイル内のデバイスの CLI ユーザ名、CLI パスワード、CLI イネーブルパスワード、および CLI タイムアウト値のフィールドに値を入力しないと、Prime Infrastructure は、そのデバイスの設定を変更したり、デバイスのソフトウェアイメージを更新したり、その他の便利な機能を実行したりできません。

これは、完全なデバイス インベントリの収集にも影響します。Prime Infrastructure で部分的なインベントリ収集を行うには、CSV ファイルの少なくとも次のフィールドの値を指定する必要があります。

- デバイスの IP アドレス
- SNMP バージョン（SNMP version）
- SNMP 読み取り専用コミュニティ ストリング（SNMP read-only community strings）
- SNMP 書き込みコミュニティ ストリング（SNMP write community strings）
- SNMP 再試行値(SNMP write community strings)
- SNMP タイムアウト値

Prime Infrastructure で完全なインベントリ収集を行うには、[プロトコル（Protocol）] フィールドの値と、指定したプロトコルに対応するフィールドの値も指定する必要があります。たとえば、[プロトコル（Protocol）] フィールドに値 **SNMPv3** を指定する場合は、サンプル CSV ファイルの [SNMPv3] フィールドの値（SNMPv3 のユーザ名と認証パスワードなど）も指定する必要があります。

CSV ファイルでクレデンシャル プロファイルを指定し、クレデンシャルをデバイスのセットに適用できます。クレデンシャル プロファイルを指定し、CSV ファイルに手動で値を入力すると、手動で入力されたクレデンシャルとクレデンシャルプロファイルの組み合わせに基づいてデバイスが管理され、手動で入力されたクレデンシャルの優先順位が高くなります。たとえば、手動で入力した SNMP クレデンシャルに加えて SNMP および Telnet のクレデンシャルを

含むクレデンシャル プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP クレデンシャルとクレデンシャル プロファイル内の Telnet クレデンシャルに基づいて管理されます。

インポートする CSV ファイルにユーザ定義フィールド（UDF）パラメータが含まれている場合は、CSV ファイルをインポートする前にこれらの UDF パラメータを必ず追加する必要があります。これを行うには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[ユーザ定義フィールド（User Defined Fields）]** を選択し、各 UDF パラメータを追加します。CSV ファイルの [UDF] 列は、CSV テンプレートに示されているように、**UDF:** で始まる必要があります。UDF フィールドパラメータには、特殊文字 : ; および # を使用しないでください。

（注） 一括インポート時には、CSV ファイルに IP アドレスとクレデンシャルプロファイル名の情報のみを含める必要があります。

# 手動によるデバイスの追加（新規デバイスタイプまたはデバイス シリーズ）

新しいデバイス タイプを追加して、それらの設定をデバイスのグループに適用する前にテストするには、次の手順に従います。

**ステップ 1** [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択します。

**ステップ 2** [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

**ステップ 3** [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

（注） IE1k デバイスを追加する場合は、[デバイスの追加（Add Device）] ダイアログ ボックスに **HTTP/HTTPS パラメータ**を入力する必要があります。この情報を無視すると、デバイスは [収集の部分的な失敗（Partial Collection Failure）] 状態に移行します。

（注） コンプライアンス ポリシーを使用するデバイスには、Telnet/SSH 情報が必須です。Telnet/SSH（60 秒）と SNMP（10 秒）のデフォルト タイムアウトがネットワーク遅延に基づいてデバイスにより異なる場合でも、デバイスを構成できます。

[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [SSH の厳格なホスト チェック キー（Strict host check key for SSH）] チェック ボックスを選択して、追加したデバイスの SSH キーの検証を強制することができます。これにより、Telnet/SSH のパラメータの下でアルゴリズムおよび SSH キーを指定することができます。

デバイスを追加するときにアルゴリズムと SSH キーを手動で指定しない場合は、[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [最初の使用で SSH キーを信頼する（Trust SSH key on first use）] チェック ボックスを選択します。その最初の通信中にデバイスから送信された SSH キーは、信頼されデバイスのクレデンシャルに追加されます。この保存されたキーは、その後デバイスが追加されたときに自動入力され、検証に使用されます。

**ステップ 4** （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

UCS シャーシなどのデバイスの HTTPS クレデンシャルを確認するには、デバイスから証明書を取得して Prime Infrastructure のトラストストアに追加してください。Prime Infrastructure のトラストストアに証明書を追加するには、次のコマンドを使用します。

- ncs key importcacert <*name*> <*certificate filename*> repository <*name of repository*>
- ncs stop
- ncs start

**ステップ 5** [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

（注） ユーザ定義フィールド（UDF）パラメータが新しいデバイスに使用可能になるのは、最初に **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [ユーザ定義フィールド（User Defined Fields）]** を選択して UDF パラメータを追加した場合のみです。UDF フィールド パラメータには、特殊文字 : ; および # を使用しないでください。

（注） NCS 2000 デバイスの場合、[シングルセッション TL1 を有効にする（Enable Single Session TL1）] の設定はリリース 11.0 以降を実行しているデバイスに対してのみ有効です。

（注） Prime Infrastructureは、デフォルトではUCSを自己署名証明書で承認しません。ユーザがこれを手動で有効にするには、*/opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def*ファイルに次の行を追加します。

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

# 仮想デバイス コンテキストの追加

Prime Infrastructure では、Cisco NX-OS ソフトウェアが仮想デバイス コンテキスト（VDC）をサポートします。これにより、単一のデバイスを複数の論理デバイスにパーティション分割して、障害の分離、管理の分離、アドレス割り当ての分離、サービス差別化ドメイン、および適応型リソース管理を実現します。VDC では、デバイス レベルでスイッチを仮想化できます。VDC は、実行中の独自のソフトウェア プロセスを保持する個別の論理エンティティとして実行し、独自の設定を持ち、管理者によって管理されます。**VDC1**は、特別なロールを持っているデフォルト（管理）VDC です。子 VDC を設定して、リソースを割り当てることができます。

Prime Infrastructure は、Cisco NX-OS ソフトウェア リリース 6.2(12) 以降を実行するデバイスで Cisco Nexus のすべてのスイッチ機能を管理します。

デフォルト VDC を備えたデバイスを追加するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

**ステップ 2** [デバイスの追加（Add Device）] ドロップダウンリストから、[デバイスの追加（Add Device）] を選択します。

**ステップ 3** さまざまなタブで必要な設定を指定します。

特定のパラメータの説明を表示するには、**[?]** アイコン上にカーソルを置きます。

**ステップ 4** （任意）デバイスを追加する前に、[クレデンシャルの確認（Verify Credentials）] をクリックして、入力したクレデンシャルが有効であることを確認します。

**ステップ 5** [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

インベントリ収集が正常に実行された後に、デフォルトの VDC を備えたデバイスが追加されます。その後、子 VDC が自動的に追加され、その設定が Prime Infrastructure データベースに保存されます。

# Prime Infrastructure への Meraki デバイスの追加

Cisco Prime Infrastructure では、すべてのアクセスポイント、セキュリティアプライアンス、およびスイッチのスイッチをモニタできます。Cisco Prime Infrastructure は、SNMP プロトコルを使用して、モニタリングとインベントリの両方の目的で、クラウドから、そのデバイスに関する情報を抽出します。

Cisco Meraki を Cisco Prime Infrastructure に統合するには、次のものが必要です。

- ダッシュボードで SNMP を有効にする
- Cisco Prime Infrastructure サーバへの [追加 (Add)] ダッシュボードの追加
- 接続の確認

プライムデバイスをプライムインフラストラクチャに追加するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）][デバイス管理（Device Management）][ネットワーク デバイス（Network Devices）]** を選択します。

**ステップ 2** [ネットワーク デバイス（Network Devices）] テーブルの上にある + アイコンをクリックし、**[デバイスの追加（Add Device）]** を選択します。

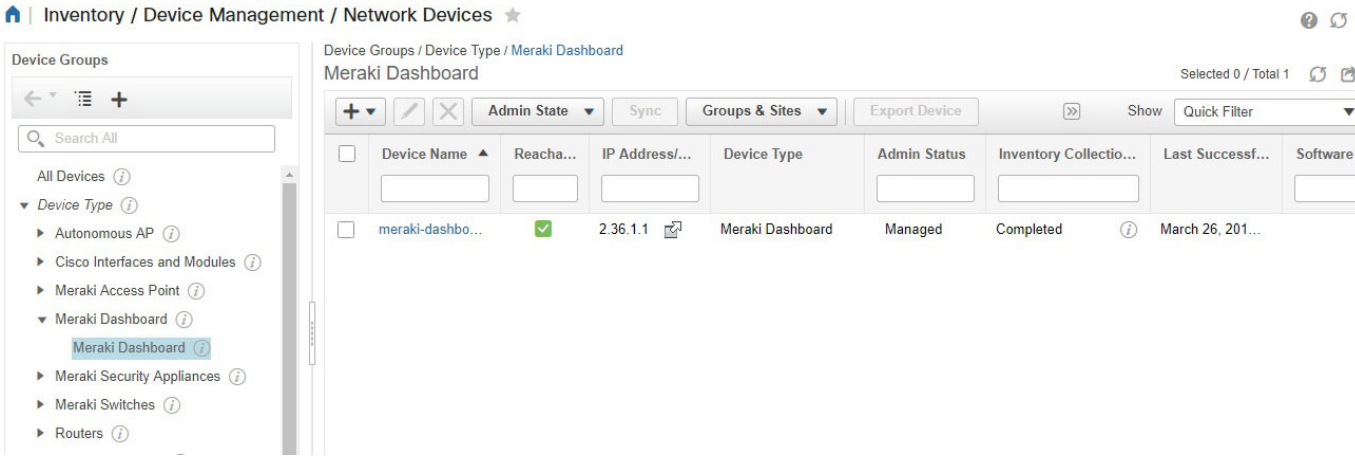
**ステップ 3** Meraki ダッシュボードの **IP アドレス**または **DNS 名**を入力します。

**ステップ 4** **[デバイスの追加 (Add Device )]** 画面で SNMP v2/v3 クレデンシャルを入力します。

**ステップ 5** （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

**ステップ 6** **[追加（Add）]** をクリックして、指定した設定でデバイスを追加します。デバイスの詳細が右側のペインに表示されます。次のようなものがあります。

- Device Name
- 到達可能性/ステータス
- IP アドレス/DNS名
- デバイスタイプまたはモデル
- MAC address
- クライアント数
- シリアル番号
- メッシュ ステータス
- ネットワーク名。




このダッシュボードは、複数のデバイスを構成するための単一の設定点のままです。Ciscoプライムを使用すると、デバイスのIPアドレスの横にデバイスリンクを含めることで、特定のデバイスに簡単にアクセスできます。これらのリンクにより、ブラウザウィンドウが起動します。これにより、管理者は、特定のデ

バイスに関する包括的な情報を抽出するのに役立つ、作成者のダッシュボードのデバイスに対する権限を得ることができます。

（注） 必要なアクセスポイント、スイッチ、およびセキュリティアプライアンスを表示するには、[**ネットワークデバイス (Network Devices )**] ページのグループセレクタ/オブジェクトセレクタから適切なデバイスグループを選択する必要があります。

# ワイヤレス コントローラを追加するための前提条件

Prime Infrastructure にワイヤレス デバイスを追加する場合は、次の情報に注意してください。

- Prime Infrastructure からワイヤレス コントローラを取り外すと、そのコントローラに関連付けられたアクセスポイントも削除する必要があるかどうかを確認する警告メッセージが表示されます。
- IPSec を使用する GRE リンク、または複数のフラグメントを含むより下位の MTU リンクを使用してコントローラを追加する場合は、[Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] と [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を調整する必要があります。これらの値が高すぎると、コントローラが Prime Infrastructure に追加されないことがあります。

  [Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] または [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を調整するには、Prime Infrastructure サーバを停止し、**[管理（Administration）]** > **[設定（Settings）]** > **[ネットワークとデバイス（Network and Device）]** > **[SNMP]** を選択し、[Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] と [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を 50 以下に編集します。
- ワイヤレス コントローラを追加していて、「スパーステーブルがサポートされていません（Sparse table not supported）」というエラー メッセージが表示された場合は、再試行する前に、Prime Infrastructure と WLC の両方の互換バージョンを実行していることを確認してください。2 つの製品の互換バージョンの詳細については、Cisco.com で Prime Infrastructure の『Cisco Wireless Solutions Software Compatibility Matrix』のエントリを参照してください。
- Prime Infrastructure は、追加するコントローラのトラップ受信機として機能します。コントローラ上では、802.11 Disassociation、802.11 Deauthentication、および 802.11 Authenticated というトラップが有効になっています。
- 新しいコントローラを追加すると、Prime Infrastructure が新しいコントローラとの通信を試行しているときに、コントローラの到達可能性が「不明（Unknown）」としてリストされます。コントローラとの通信が成功すると、コントローラの到達可能性が「到達可能（Reachable）」または「ping到達可能（Ping Reachable）」に変わります。
- コンプライアンスを有効にすると、WLC は次の理由により、部分的なインベントリ収集状態に移行します。

- CLI クレデンシャルに読み取り/書き込み権限がない。
- 同期時に WLC が接続を閉じる。
- WLC が設定したタイム アウト時間内に応答しない。

- 複数のコントローラのクレデンシャルをまとめて更新するには、**[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] > [ワイヤレスコントローラ（Wireless Controllers）]** を選択します。次に、更新する必要があるコントローラを選択し、[編集（Edit）] アイコンをクリックします。最後に、クレデンシャル プロファイルを選択し、[更新（Update）] または [更新と同期（Update & Sync）] をクリックします。
- また、更新するコントローラのリストを含むCSVファイルを作成して、複数のコントローラのクレデンシャルを一括して更新することもできます。1 行に 1 つのコントローラが存在することを確認します。各行には、更新するコントローラ属性のカンマ区切りリストが表示されます。
  - **[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] > [ワイヤレスコントローラ（Wireless Controllers）]** を選択します。
  - テーブルの上の ＋ アイコンをクリックします。
  - [一括インポート（Bulk Import）] を選択し、CSV ファイルを参照します。

# 追加されたデバイスの検証と問題のトラブルシューティング

ディスカバリ プロセスをモニタするには、次の手順を実行します。

**ステップ 1** ディスカバリ プロセスを確認するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** を選択します。

**ステップ 2** ジョブ インスタンスを展開して詳細を表示し、次の各タブをクリックして、そのデバイスのディスカバリに関する詳細を表示します。

- [到達可能（Reachable）] : ICMP を使用して到達したデバイス。デバイスは到達可能ですが、モデル化されていない可能性があります。これは、ディスカバリを使用したデバイスの追加 （3 ページ）で示されているように、さまざまな理由で発生する可能性があります。このタブの情報から問題がないか確認してください。
- [フィルタ済み（Filtered）] : カスタマイズされたディスカバリ設定に従ってフィルタ処理されたデバイス。
- [ping で到達可能（Ping Reachable）] : ICMP ping で到達可能だったものの、SNMP を使用して通信できなかったデバイス。これには、複数の理由（無効な SNMP クレデンシャル、SNMP がデバイスで有効になっていない、ネットワークで SNMP パケットが廃棄されたなど）が原因が考えられます。

- [到達不能（Unreachable）]：障害により ICMP ping に応答しなかったデバイス。
- [不明（Unknown）]：Prime Infrastructure は、ICMP または SNMP によってデバイスに接続できません。

（注） TL1 プロトコルを使用するデバイスの場合は、ノード名にスペースが含まれないようにしてください。そうでない場合、接続障害が発生します。

**ステップ 3** デバイスが正常に Prime Infrastructure に追加されたことを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。次のアクションを実行します。

- 追加したデバイスがリストに表示されていることを確認します。Prime Infrastructure がデバイスから収集したデバイス設定とソフトウェア イメージを表示するには、デバイス名をクリックします。
- [インベントリ収集ステータス（Inventory Collection Status）] フィールドの上にマウス カーソルを合わせ、表示されるアイコンをクリックすると、デバイスから収集された情報の詳細が表示されます。
- デバイスの到達可能性ステータスの列と管理者ステータスの列を確認します。デバイスの到達可能性状態と管理状態 （17 ページ）を参照してください。

Prime Infrastructure がデバイスをサポートしていることを確認するには、『*Cisco Prime Infrastructure Supported Devices*』を参照してください。

# デバイスの到達可能性の状態および管理ステータスの確認

次の手順を実行して、Prime Infrastructure がデバイスと通信できるか（到達可能性の状態）や、そのホストを管理しているか（管理ステータス）を判断します。また、管理ステータスでは、デバイスが Prime Infrastructure によって正常に管理されているかどうかの情報も提供されます。

**ステップ 1** **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

**ステップ 2** [ネットワーク デバイス（Network Devices）] テーブルでデバイスを確認します。

a) [表示（Show）] ドロップダウン リスト（テーブルの右上）から [クイック フィルタ（Quick Filter）] を選択します。

b) [デバイス名（Device Name）] 列の下にあるテキスト ボックスにデバイスの名前（またはその一部）を入力します。

**ステップ 3** [到達可能性（Reachability）] 列と [管理ステータス（Admin Status）] 列の情報を確認します。これらの状態の説明については、デバイスの到達可能性状態と管理状態 （17 ページ）を参照してください。

# デバイスの到達可能性状態と管理状態

**デバイスの到達可能性状態**：Prime Infrastructure が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

**表 *2*：デバイスの到達可能性状態**

| アイコン | デバイスの到達可能性状態 | 説明 | トラブルシューティング |
|---|---|---|---|
|  | 到達可能 | Prime Infrastructure は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。 | — |
|  | ping 到達可能 | Prime Infrastructure は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。 | ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Prime Infrastructure の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。 |
|  | 到達不能 | Prime Infrastructure は、ping を使用してデバイスに到達できません。 | 物理デバイスが動作中でネットワークに接続されていることを確認します。 |
|  | 不明 | Prime Infrastructure は、デバイスに接続できません。 | デバイスをチェックします。 |

**デバイスの管理状態**：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

**表 *3*：デバイスの管理状態**

| デバイスの管理状態 | 説明 | トラブルシューティング |
|---|---|---|

| | | |
|---|---|---|
| 管理対象 | Prime Infrastructure は、デバイスを積極的にモニタしています。 | 該当なし。 |
| メンテナンス | Prime Infrastructure は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。 | デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （18 ページ）を参照してください。 |
| 管理対象外 | Prime Infrastructure は、デバイスをモニタしていません。 | [ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。<br>• デバイス SNMP クレデンシャルが間違っている。<br>• Prime Infrastructure 展開がライセンスで許可されているデバイスの数を上回っている。<br>• デバイスがスイッチ パス トレース専用になっている。<br>デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。 |
| 不明 | Prime Infrastructure は、デバイスに接続できません。 | デバイスをチェックします。 |

# デバイスのメンテナンス状態の切り替え

デバイスの管理ステータスが [メンテナンス（Maintenance）] に変更されると、Prime Infrastructure はデバイスのインベントリ変更用のポーリング操作も、デバイスで生成されたトラップまたは Syslog の処理も行わなくなります。ただし、Prime Infrastructure は引き続き既存のリンクを維持し、デバイスの到達可能性をチェックします。

すべての管理状態および対応するアイコンのリストについては、デバイスの到達可能性状態と管理状態 （17 ページ）を参照してください。

**ステップ 1** [ネットワーク デバイス（Network Devices）] テーブルで、**[管理状態（Admin State）] > [メンテナンス ステートに設定（Set to Maintenance State）]** の順に選択します。

**ステップ 2** デバイスを完全な管理状態に戻すには、**[管理状態（Admin State）] > [管理対象状態に設定（Set to Managed State）]** の順に選択します。

（注） [メンテナンス状態をスケジュール（Schedule Maintenance State）] および [管理状態をスケジュール（Schedule Managed State）] オプションを使用して、特定の日時にメンテナンスを行い、特定の日時に管理状態に戻すようにデバイスをスケジュールすることもできます。

# デバイス パラメータの編集

[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択して、単一のデバイスまたは複数のデバイスのデバイス パラメータを編集できます。

デバイス パラメータを編集するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

**ステップ 2** 単一のデバイスまたは複数のデバイスを選択し、[編集（Edit）] アイコンをクリックします。

9台を超えるデバイスを編集すると、[**ジョブダッシュボード (Job Dashboard )**] ページでジョブがトリガーされます。一括編集のステータスがそのページに表示されます。

**ステップ 3** 必須パラメータを更新します。

**ステップ 4** 選択したすべてのデバイスのパラメータを更新する場合は [更新（Update）] をクリックし、更新されたパラメータでデバイスを更新して同期する場合は [更新&同期（Update & Sync）] をクリックします。

# デバイスの同期化

Prime Infrastructure データベースをデバイスで実行中の設定と同期するために、インベントリ収集を実行できます。

デバイスを同期するには、次の手順に従います。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

**ステップ 2** Prime Infrastructure データベースに保存されている設定と同期する設定を持つデバイスを選択します。

**ステップ 3** [同期（Sync）] をクリックします。

（注） 同期されたデバイスがデフォルト/管理 VDC の場合は、すべての子 VDC のすべての設定が自動的に同期され、その設定が Prime Infrastructure データベースで更新されます。管理 VDC の同期により、ハードウェアで新しく追加された VDC もユーザ インターフェイスに追加されます。また、ハードウェアで削除された VDC はユーザ インターフェイスから削除されます。

# スマート インベントリ

スマート インベントリでは、デバイスの commitID が変更されない限り、限られた情報のみが収集されるようにすることができます。変更があった場合は、全情報の収集が行われます。スマート インベントリの目的は、Prime Infrastructure とデバイスの間で転送されるデータの量をスマートな方法で削減することです。Prime Infrastructure は主要なインベントリ収集を行い、デバイスの設定に変更があった場合のみ、完全なコンフィギュレーションアーカイブを行います。デバイスの実行コンフィギュレーションに変更がない場合は、イメージ、フラッシュ、ファイル、インターフェイス ステータスなど、物理的な情報のみがデバイスから収集されます。デバイスの実行コンフィギュレーションに変更がない場合は、コンフィギュレーション アーカイブはトリガーされません。

スマート インベントリを有効にするには、次の手順を実行します。

**ステップ 1** **[管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [スマート インベントリ（Smart Inventory）]** を選択します。

**ステップ 2** [スマートインベントリをグローバルで有効化（Enable Smart Inventory Globally）] チェック ボックスを選択します。サポートされているすべてのデバイスが一覧表示されます。

（注） スマートインベントリをデバイスごとに有効化/無効化することもできます。必要なデバイスを選択し、[有効化（Enable）] ボタンまたは [無効化（Disable）] ボタンをクリックします。

# NAM HTTP/HTTPS クレデンシャルの追加

ネットワークのモニタリングに Cisco ネットワーク解析モジュール（NAM）を使用している場合は、Prime Infrastructure がそのモジュールからデータを取得できるように、HTTPS クレデンシャルを追加する必要があります。これは、ほとんどの保証機能は NAM データに依存して機能するため、ライセンス済みの保証機能を持つユーザに対して特に重要です。

Prime Infrastructure は、HTTP（または HTTPS）を介して NAM を直接ポーリングしてデータを収集します。このタイプのポーリングでは、Prime Infrastructure が各 NAM の HTTP クレデンシャルを保存する必要があります。SNMP コミュニティ ストリングおよび Telnet/SSH クレデンシャルとは異なり、ディスカバリ プロセス中に NAM HTTP クレデンシャルを入力できませ

ん。モジュールが検出された後またはインベントリに追加された後に実行できるのは、NAM HTTP クレデンシャルを指定することだけです。

単一の NAM の HTTP クレデンシャルを追加するには、次の手順を実行します。このタスクを、Prime Infrastructure でデータを収集するすべての NAM に繰り返すことができます。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] > [デバイスタイプ（Device Type）] > [Ciscoインターフェイスおよびモジュール（Cisco Interfaces and Modules）] > [ネットワーク解析モジュール（Network Analysis Modules）]** の順に選択します。

**ステップ 2** NAM の 1 つを選択して、[Edit] をクリックします。

**ステップ 3** [デバイスの編集（Edit Device）] ウィンドウの、[HTTP パラメータ（Http Parameters）] で以下を行います。

- [プロトコル（Protocol）] : HTTP プロトコルに HTTP または HTTPS を選択します。TCP ポートは、選択したプロトコルのデフォルト ポートに自動的に変更されます。
- [TCP ポート（TCP Port）] : デフォルトを上書きする場合は、別の TCP ポートを入力します。
- [ユーザ名（Username）] : HTTP または HTTPS 経由で NAM にアクセスできるユーザの名前を入力します。
- [Password] : 入力したユーザ名のパスワードを入力します。
- [パスワードの確認（Confirm Password）] : 確認するパスワードをもう一度入力します。

**ステップ 4** [更新（Update）] を選択します。

# CSV ファイルへのデバイス情報のエクスポート

デバイス リストをファイルにエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。次に、選択したパスワードを使用してファイルが圧縮され、暗号化されます。エクスポートしたファイルには、デバイスの SNMP クレデンシャル、CLI 設定、および地理的座標に関する情報が含まれています。エクスポートされたファイルにはデバイスのクレデンシャルが含まれていますが、クレデンシャルのプロファイルは含まれていません。

⚠

**注意** CSV ファイルにはエクスポートしたデバイスのすべてのクレデンシャルのリストが含まれるため、十分に注意して使用してください。デバイスのエクスポートは特殊な権限を持つユーザのみが実行できるようにする必要があります。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

**ステップ 2** エクスポートするデバイスを選択し、[デバイスのエクスポート（Export Device）] を選択します（または、 をクリックして [デバイスのエクスポート（Export Device）] を選択します）。

**ステップ 3** [デバイスのエクスポート（Export Device）] ダイアログボックスで、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。ユーザはエクスポートされたファイルを開くのにこのパスワードを指定する必要があります。必要に応じて、エクスポートするCSVファイルの名前を入力します。

**ステップ 4** パスワード、確認パスワード、またはエクスポートファイル名を入力し、[エクスポート（Export）] をクリックします。ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

CSV ファイルにデバイスの詳細をエクスポートするもののデバイスのクレデンシャルは含めない場合は、設定アイコンの横にある をクリックします。この CSV ファイルには、デバイスの詳細を何件でもエクスポートできます。しかし、このCSVファイルを使用してデバイスをインポートすることはできません。

# クレデンシャルプロファイルを使用したデバイスクレデンシャルの一貫した適用

資格情報のプロファイルは、TL1、HTTP、Telnet/SSH SNMP デバイスの認証情報のコレクションです。デバイスを追加するときは、デバイスを使用する必要があります資格情報のプロファイルを指定できます。これにより、デバイス間で一貫して資格情報の設定を適用できます。

資格情報の変更、デバイスのパスワードの変更などを行う必要がある場合は、設定がプロファイルを使用するすべてのデバイスにわたって更新されるプロファイルを編集できます。

既存のプロファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）] を選択します。

## 新しいクレデンシャル プロファイルの作成

この手順を使用して、新しいクレデンシャルプロファイルを作成します。次に、そのプロファイルを使用し、製品全体か、または新しいデバイスの追加時に、クレデンシャルを一貫して適用できます。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

**ステップ 2** 既存のクレデンシャルプロファイルに必要な設定のほとんどがある場合は、それを選択し、[コピー（Copy）] をクリックします。それ以外の場合は、[追加（Add）] をクリックします。

**ステップ 3** プロファイル名と説明を入力します。名前と説明が [クレデンシャルプロファイル（Credential Profiles）] ページに表示されるため、クレデンシャルプロファイルが多くなる場合は可能な限り識別しやすい名前と説明にします。

**ステップ 4** プロファイルのクレデンシャルを入力します。このプロファイルを使用してデバイスを追加または更新すると、ここで指定した内容がそのデバイスに適用されます。

SNMP 読み取りコミュニティ ストリングは必須です。

**ステップ 5** [変更の保存（Save Changes）] をクリックします。

# 既存のデバイスへの新規または変更されたプロファイルの適用

次の手順を使用して、デバイスを一括編集し、そのデバイスが関連付けられているクレデンシャル プロファイルを変更します。この操作は、デバイスとクレデンシャル プロファイル間の既存の関連付けを上書きします。また、この操作を使用して、デバイス設定を新しい設定と同期させることもできます。

（注） この手順を実行して **[Update and Sync]** を選択する前に、プロファイルのクレデンシャル設定が正しいことを確認してください。この操作によって、デバイスは新しいプロファイルと同期します。

**ステップ 1** 次のいずれかの方法を使用して、クレデンシャル プロファイルを設定します。

- 新しいクレデンシャル プロファイルを作成するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、[追加（Add）] をクリックします。
- 既存のプロファイルを編集するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[編集（Edit）] をクリックします。

**ステップ 2** プロファイルに納得できたら、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

**ステップ 3** 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

**ステップ 4** [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから新しいクレデンシャル プロファイルを選択します。

**ステップ 5** 次のように変更を保存します。

- [更新（Update）] は、変更を Prime Infrastructure データベースに保存します。
- [更新して同期（Update and Sync）] は、変更を Prime Infrastructure データベースに保存し、デバイスの物理インベントリと論理インベントリを収集して、インベントリのすべての変更を Prime Infrastructure データベースに保存します。

# クレデンシャル プロファイルの削除

この手順で、クレデンシャル プロファイルを Prime Infrastructure から削除します。現在、プロファイルがデバイスに関連付けられている場合は、デバイスの関連付けをそのプロファイルから解除する必要があります。

**ステップ 1** 何らかのデバイスがプロファイルを使用しているかどうかを確認します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** に移動します。

b) 削除するクレデンシャル プロファイルを選択します。

c) [編集（Edit）] をクリックし、[デバイス リスト（Device List）] ページにデバイスが一覧表示されているかどうかを確認します。デバイスが一覧表示されている場合は、それらをメモします。

**ステップ 2** 必要に応じて、プロファイルからデバイスの関連付けを解除します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** に移動します。

b) 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

c) [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから [--選択--（--Select--）] を選択します。

d) 警告ダイアログボックスで[OK]をクリックし、古いプロファイルからデバイスの関連付けを解除します。

**ステップ 3** クレデンシャル プロファイルを削除するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[削除（Delete）] をクリックします。

# クレデンシャル プロファイルのエクスポートとインポート

次の手順を使用して、デバイス管理からクレデンシャルプロファイルをエクスポートおよびインポートできます。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

**ステップ 2** エクスポートするクレデンシャルプロファイルを選択し、[プロファイルの**エクスポート (Export profile)**] をクリックします。

**ステップ 3** [プロファイルのエクスポート (Export Profile)] ポップアップウィンドウで、次のクレデンシャルを入力します。

- Password
- Confirm Password
- エクスポートファイル名

**ステップ 4** [**エクスポート (Export )**] をクリックして、デバイスの csv ファイルに関連付けられたプロファイルとプロファイルを含む zip ファイルを保存します。

**ステップ 5** クレデンシャルプロファイルをインポートするには、次の手順を実行します。

**ステップ 6** Prime Infrastructure サーバにログインします。

**ステップ 7** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

**ステップ 8** **[一括インポート（Bulk Import）]** をクリックします。

**ステップ 9** [一括インポート (Bulk Import)] ポップアップで、クレデンシャルプロファイル .csv ファイルを参照して、[**インポート (import)**] をクリックします。

**注意** 一括インポート中に**Profile_associated_devices** .csv ファイルをインポートしないでください。

**ステップ 10** インポートが完了すると、クレデンシャルプロファイルの一括インポートジョブが作成されます。[Administration] [ **> Dashboard] [> Job dashboard] [> User Jobs > Credential Profile] [Bulk Import** ] の順に移動して、ジョブを確認できます。

# 簡単な管理と設定のためのデバイス グループの作成



デバイスを論理グループに編成すると、デバイスの管理、モニタリング、設定が簡素化されます。グループに操作を適用できるため、グループ化によって時間が節約され、ネットワーク全体で設定が一貫して適用されます。すべてのデバイスを同じ設定で構成できる小規模の構成では、ただ1つの一般的なデバイス グループを作成するだけで済みます。グループ化メカニズムは、サブグループもサポートしています。これらのグループは、多くの Prime Infrastructure GUI ウィンドウに表示されます。

デバイスが Prime Infrastructure に追加されると、[未定義（Unassigned）] という名前のロケーション グループに割り当てられます。多数のデバイスを管理している場合は、デバイスを他のグループに移動して、[未定義（Unassigned）] のグループ メンバーシップが大きくなりすぎないようにしてください。

# グループの仕組み

グループはアクセス制御を行いません。アクセス制御は仮想ドメインによって決まります。この違いについては、グループおよび仮想ドメイン （30 ページ） を参照してください。

特定のタイプのグループについては、関連項目 ネットワーク デバイス グループ （26 ページ） および ポート グループ （27 ページ） を参照してください。

グループに要素を追加する方法については、グループに要素を追加する方法：動的、手動、および混在グループ （29 ページ） を参照してください。

## ネットワーク デバイス グループ

次の表に、サポートされているネットワーク デバイス グループのタイプを示します。デバイス グループにはインベントリからアクセスできます。

| ネットワーク デバイス グループの種類 | メンバーシップの条件 | ユーザが作成または編集できるか |
|---|---|---|
| デバイス タイプ（Device Type） | デバイスはファミリごとにグループ化されます（たとえば、、ルータ、スイッチおよびハブなど）。各デバイス ファミリの下で、デバイスはさらにシリーズごとにグループ化されます。新しいデバイスは、適切なファミリおよびシリーズ グループに自動的に割り当てられます。たとえば、Cisco ASR 9006 は、ルータ（ファミリ）および Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ（シリーズ）に属します。<br>次の点に注意してください。<br>• デバイス タイプ グループを作成することはできません。これらはシステム定義の動的グループです。代わりに、デバイス基準を使用してユーザ定義のグループを作成し、適切なデバイス名を付けます。<br>• デバイス タイプ グループはネットワーク トポロジ マップには表示されません。<br>• [Prime Infrastructure] で検出されたサポート対象外のデバイスには [サポート対象外のシスコデバイス（Unsupported Cisco Device）] デバイスタイプが自動的に割り当てられ、**[デバイスタイプ（Device Type）] > [サポート対象外のシスコデバイスファミリ（Unsupported Cisco Device Family）]** に表示されます。 | いいえ |

| | | |
|---|---|---|
| ロケーション（Location） | ロケーション グループを使用して、ロケーションごとにデバイスをグループ化できます。デバイスを手動で追加するか、またはデバイスを動的に追加して、ロケーション グループの階層（シアター、国、地域、キャンパス、ビルディング、フロアなど）を作成できます。<br>デバイスは 1 つのロケーション グループのみに表示されるはずですが、上位レベルの「親」グループにもそのデバイスが含まれています。たとえば、ビルディングのロケーション グループに属するデバイスは、親のキャンパス グループにも間接的に属している場合があります。<br>デフォルトでは、階層の上位のロケーションが [すべてのロケーション（All Locations）] グループとなります。ロケーションに割り当てられていないデバイスはすべて、[すべてのロケーション（All Locations）] の下の [未割り当て（Unassigned）] グループに表示されます。 | はい |
| ユーザ定義（User Defined） | デバイスは、デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズして、必要なデバイスおよびロケーション基準を使用できます。<br>ユーザが作成したロケーション グループは、選択したグループ（キャンパス、建物、屋外領域、屋内区域など）に応じてワイヤレス マップと同期します。したがって、ユーザが作成したロケーション グループは **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（Site Maps）]** の下に表示され、同様に、ユーザがマップの下に作成したサイトは **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の下に階層形式で表示されます。 | あり |

## ポート グループ

次の表に、サポートされているポート グループのタイプを示します。

| ポート グループの種類 | メンバーシップの条件 | ユーザが作成または編集できるか |
|---|---|---|
| ポート タイプ（Port Type） | ポートの種類、速度、名前、または説明ごとにグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。<br>ポート タイプのグループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。 | いいえ。代わりに、ユーザ定義グループを作成します。 |

| | | |
|---|---|---|
| システム定義（System Defined） | ポートの使用状況または状態別にグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。<br><br>[リンクポート（Link Ports）]：別のシスコ デバイスまたは他のネットワーク デバイスに接続され、「VLAN」モードで動作し、VLAN に割り当てられるポート。<br><br>[トランクポート（Trunk Ports）]：シスコ デバイスまたは他のネットワーク デバイス（スイッチ、ルータ、ファイアウォール、サードパーティ デバイス）に接続され、すべてのVLANのトラフィックを伝送する「トランク」モードで動作しているポート。<br><br>[アクセスポート（Access Ports）]：エンド ホスト、IP Phone、サーバ、アクセス ポイント（AP）またはビデオ エンド ポイントに接続され、ある特定の VLAN のみのトラフィックを伝送する「アクセス」モードで動作しているポート。[未接続ポート（Unconnected Ports）]：デバイスに接続されていない、管理ステータスがダウンしている、または動作状態がダウンしているポート。<br><br>ポートのステータスがダウンすると、そのポートは[未接続ポート（Unconnected Port）] グループに自動的に追加されます。このグループ内のポートを削除することはできません。また、このグループを他のグループのサブ グループとして再作成することはできません。<br><br>システム定義のポート グループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。<br><br>（注） [WAN インターフェイス（WAN Interfaces）] はスタティックグループであるため、自動ポートの追加は適用されません。したがって、手動でグループにポートを追加する必要があります。 | いいえ。代わりに、ユーザ定義グループを作成します。 |
| ユーザ定義（User Defined） | ポート基準のカスタマイズ可能な組み合わせによってグループ化され、グループに名前を付けることができます。グループが動的でポートが条件に一致する場合は、そのグループに追加されます。 | あり |

## データセンター グループ

次の表に、サポートされているデータセンター グループのタイプを示します。

表 *4:* サポートされているデータセンター グループのタイプ

| データセンターグループのタイプ | メンバーシップの条件 | ユーザが作成または編集できるか |
|---|---|---|
| システム定義 | タイプ別にグループ化されます（データセンター、クラスタ、仮想マシン（VM）、ホスト）。<br>システム定義のデータセンター グループを作成することはできません。代わりに、デバイス基準を使用してユーザ定義のデータセンター グループを作成し、ユーザ定義グループの下にサブグループを作成します。 | いいえ。VM およびホスト用のユーザ定義グループを作成できます。 |
| ユーザ定義 | デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズし、必要なデバイス基準を使用できます。 | あり |

## グループに要素を追加する方法：動的、手動、および混在グループ

グループに要素を追加する方法は、グループが動的か、手動か、混在かによって異なります。

| デバイスの追加方法 | 説明 |
|---|---|
| 動的 | 要素がグループ基準を満たしている場合、Prime Infrastructure はグループに新しい要素を自動的に追加します。指定できるルールの数に制限はありませんが、ルールを追加するにしたがい更新のパフォーマンスに影響が及ぶ場合があります。 |
| 手動 | グループの作成時またはグループの編集時に、ユーザは手動で要素を追加します。 |
| 混合 | 要素は、動的ルールと手動追加の組み合わせによって追加されます。 |

デバイス名およびポート名の一致基準を指定する場合に * や ? などのワイルドカードを使用すると、グループ内の新しい要素を動的に追加できます。例：

- *a*：名前に文字「a」が含まれます。
- ?a*：名前の 2 番目の文字に「a」が含まれます。
- ?a：名前に含まれる文字は 2 つだけで、2 番目の文字は「a」になります。
- *a：名前の最後の文字は「a」です。

親/子のユーザ定義グループおよびロケーション グループにおけるデバイスの継承は次のとおりです。

- ユーザ定義グループ：子グループを作成する場合：

- 親グループと子グループの両方がダイナミックの場合、子グループは親グループ内のデバイスにのみアクセスできます。
- 親グループが静的で、子グループが動的である場合、子グループは親グループ外のデバイスにアクセスできます。
- 親グループと子グループが動的かつ静的である場合、子グループは親のデバイス グループからデバイスを「継承」します。

- ロケーション グループ：親グループは子のグループ デバイスを継承します。

（注） 親グループの下に作成する子グループの数に制限はありません。子グループの階層レベルにも制限はありません。

## グループおよび仮想ドメイン

グループは要素の論理コンテナですが、要素へのアクセスは仮想ドメインによって制御されます。次の例は、グループと仮想ドメインの関係を示しています。

- **SanJoseDevices** という名前のグループに 100 台のデバイスが含まれています。
- **NorthernCalifornia** という名前の仮想ドメインに 400 台のデバイスが含まれています。これらのデバイスはさまざまなグループに属しており、**SanJoseDevices** グループのデバイスが 20 台含まれています。

**NorthernCalifornia** 仮想ドメインにアクセスできるユーザは、**SanJoseDevices** グループの 20 台のデバイスにアクセスできますが、このグループ内の他の 80 台のデバイスにはアクセスできません。詳細については、デバイスへのユーザアクセスを制御するための仮想ドメインの作成を参照してください。

# ユーザ定義のデバイス グループの作成

新しいデバイス タイプ グループを作成するには、ユーザ定義グループのメカニズムを使用します。デバイス タイプ グループは Prime Infrastructure 全体で使用される特殊なカテゴリであるため、このメカニズムを使用する必要があります。作成するグループが [ユーザ定義（User Defined）] カテゴリに表示されます。

新しいグループを作成するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

**ステップ 2** [[デバイスグループ（Device Groups）]] ペインで [+]（**追加**）アイコンをクリックし、[ユーザ定義グループの作成（Create User Defined Group）] を選択します。

**ステップ 3** グループの名前と説明を入力します。他のユーザ定義デバイス タイプ グループが存在する場合、[親グループ（Parent Group）] ドロップダウン リストからグループを選択することで、そのグループを親グループとして設定できます。親グループを選択しなかった場合は、新しいグループが [ユーザ定義（User-Defined）] フォルダに配置されます（デフォルト）。

（注） グループ名に '、"、<、>、&、?、/ などの特殊文字は使用できません。

**ステップ 4** 次のように、デバイスを新しい グループに追加します。

条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。IP アドレスの特定の範囲内に入るデバイスをグループ化するには、角カッコ内にその範囲を入力します。たとえば、次を指定できます。

- IPv4-10.[101-155].[1-255].[1-255] および 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

（注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

デバイスを手動で追加する場合は、次の手順を実行します。

1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

**ステップ 5** [プレビュー（Preview）] タブをクリックしてグループのメンバーを表示します。

**ステップ 6** [保存（Save）] をクリックします。

ステップ 3 で選択したフォルダに新しいデバイス グループが表示されます。

## デバイスが属するすべてのグループの表示

デバイスが属するデバイス グループのリストを表示するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]**、または **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワーク デバイス グループ（Network Device Groups）]** を選択します。

**ステップ 2** 左側の [デバイス グループ（Device Group）] ペインの [検索（Search）] フィールドに IP アドレスまたはデバイス名を入力すると、デバイスが属するすべてのグループのリストが表示されます。

検索フィールドにグループ名を入力してグループを検索することもできます。

# ロケーション グループの作成

**ステップ 1** **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

**ステップ 2** 左側の [デバイス グループ（Device Groups）] ペインで、[追加（Add）] アイコンをクリックし、[ロケーション グループの作成（Create Location Group）] を選択します。

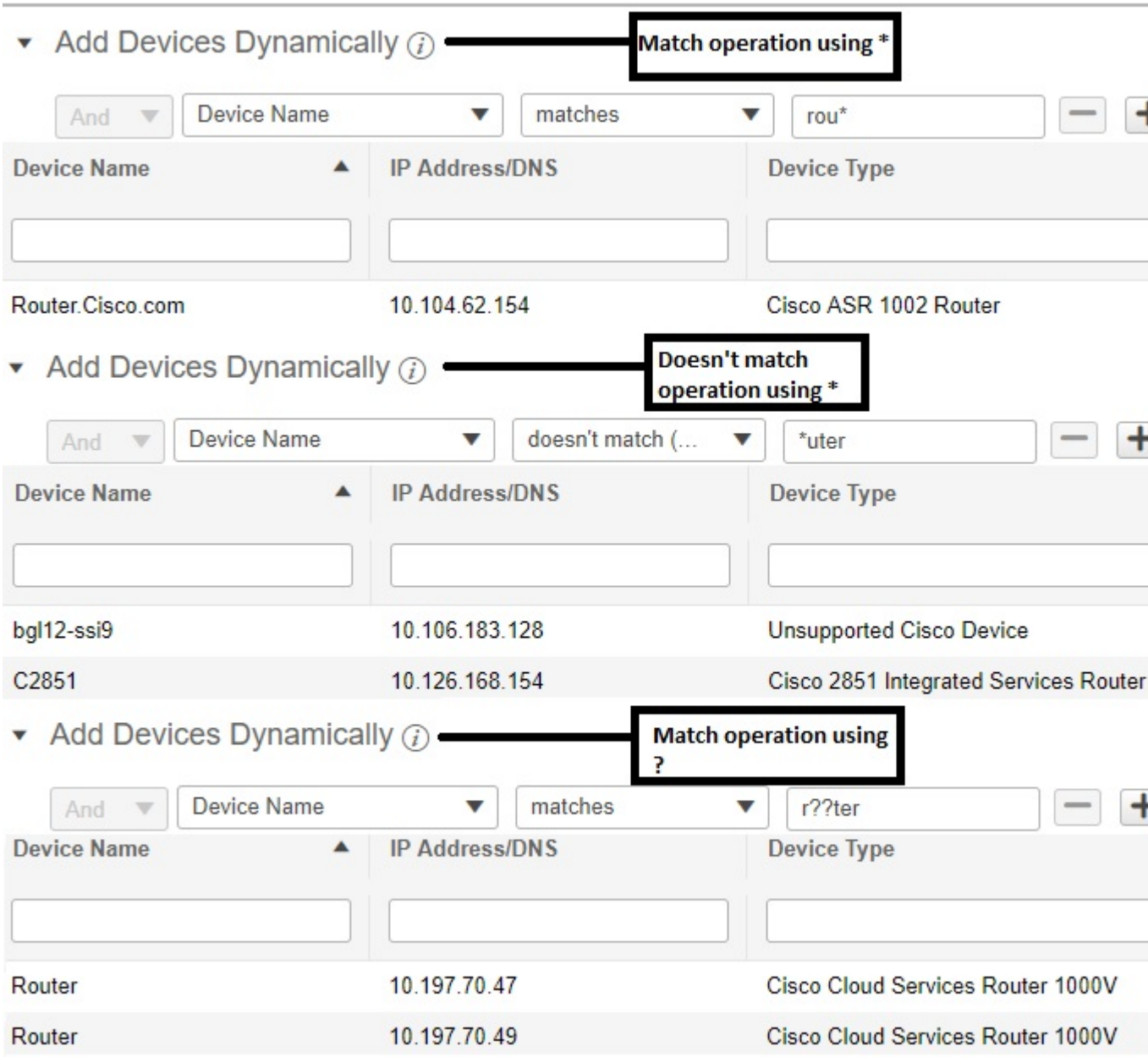
**ステップ 3** 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、[すべてのロケーション（All Locations）] のサブグループになります（つまり、[すべてのロケーション（All Locations] フォルダに表示されます）。

**ステップ 4** たとえば、特定の住所のビルディングにあるすべてのデバイスなど、地理的なロケーションに基づいてデバイス グループを作成する場合は、[地理的なロケーション（Geographical Location）] チェックボックスをオンにしてグループの GPS 座標を指定するか、または [マップの表示（View Map）] リンクをクリックし、マップ内の必要な場所をクリックします。この場合は、GPS 座標が自動的に入力されます。地理的なロケーションで定義されたロケーション グループは、Geo マップのグループ アイコンで表されます。グループに追加するデバイスは、そのグループの GPS 座標を継承します。地理的なロケーションが一連のデバイスをグループ化する主たる理由の場合は、グループに追加するデバイスに、そのグループとは異なる独自の GPS 座標を持たせないことを推奨します。

[シビックロケーション（Civic Location）] を指定する場合は、検索キーワードを手動で入力して、ドロップダウンリストからロケーションを選択します。

**ステップ 5** 特定の基準を満たしている場合にデバイスが自動的に追加されるようにするには、[デバイスを動的に追加（Add Devices Dynamically）] 領域に基準を入力します。それ以外の場合は、この領域を空欄のままにします。

ルール（[一致（matches）] および [不一致（doesn't match）]）では、ワイルドカード文字がサポートされます。次に示すように、検索テキストにワイルドカード文字（* および ?）を含めることができます。




ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

**ステップ 6** デバイスを手動で追加する場合は、次の手順を実行します。

a) [デバイスを手動で追加（Add Devices Manually）] で、[追加（Add）] をクリックします。

b) [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

**ステップ 7** [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

**ステップ 8** [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [すべてのロケーション（All Locations）]）の下に新しいロケーション グループが表示されます。

ロケーショングループを編集する場合は、次の条件を満たしている場合にグループタイプを変更できます。

- グループ タイプがデフォルト。
- グループにサブグループがない。

# CSV ファイルを使用したグループの作成

Prime Infrastructure に追加するグループのすべての属性が一覧表示されている CSV ファイルを使用してグループをインポートするには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）]**[グループ管理（Group Management）]**[ネットワーク デバイス グループ（Network Device Groups）]** を選択し、**[グループのインポート（Import Groups）]** をクリックします。

**ステップ 2** ここのリンクをクリックし、CSV ファイルのサンプル テンプレートをダウンロードします。

テンプレート内で示されているように、CSV ファイル内の必須情報は必ず保持してください。

**ステップ 3** [グループのインポート（Import Groups）] ダイアログ ボックスで [ファイルの選択（Choose File）] をクリックし、インポートするグループが含まれている CSV ファイルを選択します。

**ステップ 4** [インポート（Import）] をクリックします。

**ステップ 5** **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択し、**[グループのインポート（Import Groups）]** をクリックしてジョブのステータスを表示します。

# CSV ファイルへのグループのエクスポート

グループ情報を CSV ファイルとしてエクスポートするには、次の手順を実行します。

**ステップ 1** [Inventory] > [Group Management] > [Network Device Groups] の順に選択します。

**ステップ 2** PI または APIC EM を選択します。

**ステップ 3** **[グループのエクスポート（Export Groups）]** をクリックして、すべてのロケーション グループの詳細が含まれている CSV ファイルをローカル システムにダウンロードします。

# デバイス グループとロケーション グループへの AP の追加

## 手順の概要

1. **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。
2. 左側の [デバイスグループ（Device Groups）] ペインで、[ユーザ定義（User Defined）] または [ロケーション（Location）] の横にある展開アイコンの上にマウスのカーソルを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。
3. 名前、説明、および親グループ（該当する場合）を入力します。
4. 次のいずれかの方法で AP を追加します。
5. [プレビュー（Preview）] をクリックして、指定したルールと手動で追加した AP に基づいてグループに自動的に追加された AP を確認します。
6. [保存（Save）] をクリックします。

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。 | |
| ステップ 2 | 左側の [デバイスグループ（Device Groups）] ペインで、[ユーザ定義（User Defined）] または [ロケーション（Location）] の横にある展開アイコンの上にマウスのカーソルを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。 | |
| ステップ 3 | 名前、説明、および親グループ（該当する場合）を入力します。 | |
| ステップ 4 | 次のいずれかの方法で AP を追加します。 | • 手動：[デバイスを手動で追加する（Add Devices Manually）] の下にある [追加（Add）] をクリックし、グループに追加する AP を選択します。<br>• 動的：このポート グループに追加される前に AP が従う必要のあるルールを指定します。ダイナミック グループには AP を追加しません。Prime Infrastructure が指定されたルールに一致する AP をダイナミック グループに追加します。<br><br>デフォルト以外のロケーション グループのタイプを選択すると、AP は動的には追加されません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | [プレビュー（Preview）] をクリックして、指定したルールと手動で追加した AP に基づいてグループに自動的に追加された AP を確認します。 | |
| ステップ 6 | [保存（Save）] をクリックします。 | グループにメンバーとして「**ユニファイド AP**」または「**サードパーティ AP**」がある場合、新しいタブがデバイス ワーク センターの右側のテーブルに追加され、AP が表示されます。 |

# ポート グループの作成

ポート グループを作成するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）]** を選択します。

**ステップ 2** **[ポートグループ（Port Groups）] > [ユーザ定義（User Defined）]** から、[ユーザ定義（User Defined）] の横にある [i] アイコンの上にカーソルを置き、ポップアップウィンドウの [サブグループの追加（Add SubGroup）] をクリックします。

**ステップ 3** 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、ポート グループは [ユーザ定義（User Defined）] フォルダに配置されます。

**ステップ 4** グループに追加するためにポートが属している必要があるデバイスを選択します。[デバイスの選択（Device Selection）] ドロップダウンリストから、次を選択できます。

- [デバイス（Device）] : すべてのデバイスのフラット リストからデバイスを選択します。
- [デバイス グループ（Device Group）] : デバイス グループを選択します（[デバイス タイプ（Device Type）]、[ロケーション（Location）]、および [ユーザ定義（User Defined）] グループのリストが表示されます）。

**ステップ 5** 条件を満たしている場合にポートが自動的に追加されるようにするには、[ポートを動的に追加（Add Ports Dynamically）] 領域にその条件を入力します。それ以外の場合は、この領域を空欄のままにします。

ダイナミックグループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

**ステップ 6** デバイスを手動で追加する場合は、次の手順を実行します。

a) [ポートを手動で追加（Add Port Manually）] で、[追加（Add）] をクリックします。

b) [ポートの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

**ステップ 7** [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

**ステップ 8** [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [ユーザ定義（User Defined）]）の下に新しいポート グループが表示されます。

# ユーザ定義データセンター グループの作成

設定済みのデータセンターおよびクラスタのグループに加え、VM およびホストにユーザ定義グループを作成できます。ユーザ定義グループを作成するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティング デバイス（Compute Devices）]** を選択します。

**ステップ 2** [コンピューティング リソース（Compute Resources）] ペインで [ユーザ定義のホストおよび VM（User Defined Hosts and VMs）] を見つけ、[i]（**情報**）アイコンの上にカーソルを合わせます。

**ステップ 3** [アクション（Actions）] 領域から、[サブグループの追加（Add Subgroup）] をクリックします。

[デバイス サブグループの追加（Add Device Subgroup）] ページが開きます。

**ステップ 4** グループの名前と説明を入力し、グループを配置するフォルダを [親グループ（Parent Group）] ドロップダウン リストから選択します。

**ステップ 5** 次のように、デバイスをロケーション グループに追加します。

- 条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。

  （注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

- デバイスを手動で追加する場合は、次の手順を実行します。

  1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
  2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

**ステップ 6** [プレビュー（Preview）] タブをクリックし、グループに所属させるデバイスを表示します。

**ステップ 7** [保存（Save）] をクリックします。ステップ 4 で選択したフォルダに新しいグループが表示されます。

# ユーザ定義グループの編集

編集オプションを使用して、親グループの変更、デバイスの追加、およびデバイス ルールの変更を行うことができます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワーク デバイス グループ（Network Device Groups）]** を選択します。 | |
| ステップ 2 | 左側の [デバイス グループ（Device Groups）] ペインで、編集するグループの名前をクリックします。 | |
| ステップ 3 | [編集（Edit）] をクリックして、詳細を変更します。 | ロケーション グループを編集しているときに、次に該当する場合はグループ タイプをキャンパスに変更できます。<br>• グループ タイプがデフォルト。<br>• グループにサブグループがない。 |
| ステップ 4 | [プレビュー（Preview）] をクリックして、更新されたデバイスの詳細を表示します。 | |
| ステップ 5 | [保存（Save）] をクリックして、更新されたデバイスの詳細を保存します。 | |

# グループのコピーの作成

グループの複製を作成すると、Prime Infrastructure はデフォルトでそのグループに **CopyOf***group-name* という名前を付けます。名前は必要に応じて変更できます。

グループを複製するには、次の手順を実行します。

**ステップ 1** **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

**ステップ 2** 左側の [デバイス グループ（Device Groups）] ペインから、グループを選択します。

**ステップ 3** コピーするデバイス グループを見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

**ステップ 4** [グループの複製（Duplicate Group）] をクリックし（この時点では変更を加えない）、[保存（Save）] をクリックします。Prime Infrastructure によって **CopyOf***group-name* という新しいグループが作成されます。

**ステップ 5** ユーザ定義のデバイス グループの作成 （30 ページ）とロケーション グループの作成 （32 ページ）の説明に従ってグループを設定します。

**ステップ 6** [プレビュー（Preview）] タブをクリックし、グループメンバーを調査して、グループの設定を確認します。

**ステップ 7** [保存（Save）] をクリックして、グループを保存します。

# ユーザ定義グループおよびロケーション グループのコピー

任意のユーザ定義のグループまたはロケーション グループを [グループの複製（Duplicate Group）] オプションを使用して複製できます。複製したグループには、元のグループのすべての値が含まれており、これらの値は変更できます。自動入力されたグループ名には、デフォルトで「CopyOf」のプレフィックスが追加されます。名前は必要に応じて変更できます。

子グループを複製すると、同じ親グループに子グループのコピーが作成されます

親グループを複製すると、それぞれの子グループのコピーが作成されます。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。 | |
| **ステップ 2** | 左側の [デバイス グループ（Device Groups）] ペインで、複製するデバイス グループを見つけます。グループの名前の横にある [i] アイコンをクリックし、ポップアップ メニューを表示します。 | |
| **ステップ 3** | [グループの複製（Duplicate Group）] をクリックし、グループの詳細情報を更新します。 | |
| **ステップ 4** | [プレビュー（Preview）] をクリックし、複製グループの詳細情報を表示します。 | |
| **ステップ 5** | [保存（Save）] をクリックし、複製グループを保存します。 | |

# メンバーがいないグループの非表示

デフォルトでは、グループにメンバーが存在しなくても、Prime Infrastructure は Web GUI にグループを表示します。管理者権限を持つユーザが、この設定を変更して空のグループが非表示になる、つまり Web GUI に表示されないようにすることができます。（非表示グループは Prime Infrastructure から削除されません）。

**ステップ 1** **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [グループ化（Grouping）]** を選択します。

**ステップ 2** [メンバーが存在しないグループの表示（Display groups with no members）] をオフにし、[保存（Save）] をクリックします。

グループやデバイスが多数ある場合は、[メンバーが存在しないグループの表示（Display groups with no members）]チェックボックスをオンのままにすることをお勧めします。これをオフにすると、システムのパフォーマンス速度が低下します。

# グループの削除

削除するグループにメンバーが含まれていないことを確認します。メンバーが含まれている場合、Prime Infrastructure で操作を続行することはできません。

**ステップ 1** **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

**ステップ 2** 削除するデバイス グループを左側の [デバイス グループ（Device Groups）] ペインで見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

**ステップ 3** [グループの削除（Delete Group）] をクリックし、[OK] をクリックします。

# コンピューティング リソース グループの作成

データセンターやクラスタなどのコンピューティング サービスの設定済みグループの他に、UCS サーバ、ホスト、および VM にユーザ定義グループを作成できます。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **[インベントリ（Inventory）] > [コンピューティング デバイス グループ（Compute Device Groups）]** を選択します。 | |
| **ステップ 2** | 左側の [コンピューティング リソース（Compute Resources）] で、**[ユーザ定義の UCS（User Defined UCS）]** または **[ユーザ定義のホストおよび VM（User Defined Hosts and VMs）]** の横にある展開アイコンの上にマウスを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。 | |
| **ステップ 3** | グループ名と説明を入力し、必要に応じて親グループを選択します。 | |
| **ステップ 4** | [デバイスを動的に追加（Add Devices Dynamically）] ペインで、グループ内のデバイスに適用するルールを指定します。 | |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 5** | [デバイスを手動で追加（Add Devices Manually）] ペインで、グループに割り当てるコンピューティング リソースを選択します。 | |
| **ステップ 6** | [プレビュー（Preview）] をクリックして、指定したルールと手動で追加したデバイスに基づいてグループに自動的に追加されたデバイスを確認します。 | |
| **ステップ 7** | **[保存（Save）]** をクリックして、指定した設定でデバイス グループを追加します。 | |